IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An information processing apparatus comprising:

a content data storage area configured to store content data and content management information for managing the content;

a first controlling means for controlling reading/writing of content data from/to the content data storage area;

a second control means independent of the first control means for decrypting and executing an encrypted program supplied from the first control means, and, to supply the result of the program execution to the first control means; and

the first control means controlling the reading/writing from/to the content data storage area based on the program execution result supplied from the second control means, wherein the second control means performs a computation to determine whether the content management information has been falsified by computing a current hash value of the management information and comparing the computed hash value with a past hash value computation of the management information.

Claim 2 (Previously Presented): The apparatus as set forth in Claim 1, wherein:

the first control means controls the second control means program to execute a predetermined computation based on the management information.

Claim 3 (Previously Presented): The apparatus as set forth in Claim 1, wherein:

the first control means is a data processor;

the content data storage area is a hard disc; and

the second control means is a data processor incorporated in a semiconductor IC other than the data processor of the first control means.

Claim 4 (Previously Presented): An information processing apparatus comprising:

a storage medium configured to store content data and corresponding content management information;

a process controller employing an instruction set to control reading/writing of content data from/to the storage medium; and

a program execution controller provided in a semiconductor chip independent of the process controller and which is supplied with an encrypted program from the process controller decrypts the program and supplies the result of the program execution to the process controller;

the process controller controlling storage or read of the content data into or from the storage medium based on the result of the program execution by the program execution controller; and

the program execution controller being adapted so that its internal operations cannot be confirmed from outside the semiconductor ship, and, configured to perform a computation for checking any falsification made to the content management information.

Claims 5-8 (Canceled).

Claim 9 (Previously Presented): An information processing apparatus comprising:

an input configured to receive content data;

a content data storage area configured to store content data supplied from the input means;

means for compressing, in accordance with a first data format, the content data stored in the content data storing means;

means for encrypting, in accordance with the first data format, the data stored in the content data storing means; and

means for controlling storage or read, into or from the content data storing means, of the content data compressed by the compressing means and encrypted by the encrypted means;

wherein the compressing means compresses, or the encrypting means encrypts, data supplied in a format other than the first format from the input means, in accordance with the first data format.

Claim 10 (Previously Presented): The apparatus as set forth in Claim 9, wherein the compressing means compresses, or encrypting means encrypts, data supplied from the input means in different formats in one of a plurality of predetermined data formats, and utilizes a predetermined common compressing or encrypting format for outputting content data read from the content data storing means to a predetermined apparatus.

Claims 11-13 (Canceled).

Claim 14 (Previously Presented): A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer, the program causing the information processing apparatus to implement a method, comprising:

inputting data;

storing the input data;

compressing the stored data in a predetermined manner;

encrypting the stored data in a predetermined manner; and

controlling reading/writing of the compressed and encrypted data;

wherein the compressing means compresses, or the encrypting means encrypts, data supplied in a format other than the first format from the input means, in accordance with the first data format.

Claim 15-19 (Canceled).

Claim 20 (Previously Presented): An information processing method, comprising:

inputting content data and identification information of the content data;

storing the content data into a storage medium;

holding, as a usage rule file, the identification information of the stored content data;

performing a computation with a hash function applied to the identification information;

storing the result of the computation; and

comparing the result of the computation with a past computation result stored at the storing step to inhibit, when there is coincidence between the computation results, copy or move of the content data stored in the storage medium.

Claim 21 (Canceled).

Claims 22 (Currently Amended): An information processing apparatus comprising:

an interface configured to transmit and receive data to and from other apparatus;

a first memory area configured to store a predetermined lock key and save key;

authentication means for employing the lock key held in the memory when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;

means for encrypting the communication key with the save key; and

a second memory area configured to store the data received via the interface and having been encrypted with the communication key correspondingly to the communication key encrypted by the encrypting means.

Claim 23 (Previously Presented): The apparatus as set forth in Claim 22, further comprising:

an encryption key decrypting means for decrypting the communication key stored in the second memory area using the save key; and

means for decrypting the data stored in the second memory area.

Claim 24 (Previously Presented): An information processing apparatus comprising:

an interface via which data is transferred between the apparatus and a portable device or server connected to the apparatus;

a memory configured to hold a predetermined master key and save key;

an authentication program which uses, when the data is to be transferred to or from the portable device or server, the master key stored in the memory to make a mutual authentication with the portable device or server to generate a communication key;

an encryption decryption program to decrypt, with the communication key, an encryption key with which the content data transmitted from the portable device or server has been encrypted and encrypt the encryption key with the save key;

a storage medium configured to store the content data received via the interface and encrypted with the communication key in correspondence with the encryption key encrypted with the save key;

an encryption key decryption program to decrypt, with the save key, the encryption key stored in the storage medium; and

a data decryption program to decrypt content data stored in the storage medium with the encryption key encrypted by the encryption decryption program.

Claim 25 (Canceled).

Claim 26 (Previously Presented): An information processing method, comprising:

transferring data between the apparatus and a portable device or server connected to the apparatus;

holding predetermined master key and save key;

mutually authenticating with the portable device or server, when data is to be transferred to or from the portable device or server, using the master key to generate a communication key;

decrypting, with the communication key, an encryption key with which the content data transmitted from the portable device or server has been encrypted and encrypting the encryption key with the save key;

storing the content data received via the interface and encrypted with the communication key in correspondence with the encryption key encrypted with the save key;

decrypting, with the save key, the encryption key stored in the storage medium at the storing step; and

decrypting content data stored in the storage medium with the encryption key decrypted at the encryption decrypting step.

Claim 27 (Currently Amended): A program storage medium having recorded therein a program intended for execution by an information processing apparatus and readable by a computer to implement a method, comprising:

transferring data between the apparatus and a portable device or server connected to the apparatus;

holding predetermined master key and save key;

mutually authenticating with the portable device or server, when data is to be transferred to or from the portable device or server, using the master key to generate a communication key;

decrypting, with the communication key, an encryption key with which the content data transmitted from the portable device or server has been encrypted and encrypting the encryption key with the save key;

storing the content data received via the interface and encrypted with the communication key in correspondence with the encryption key encrypted with the save key;

decrypting, with the save key, the encryption key stored in the storage medium at the storing step; and

decrypting content data stored in the storage medium with the encryption key decrypted at the encryption decrypting step.

~~transmitting and receiving data to and from other apparatus;~~

~~holding a predetermined lock key and save key;~~

~~using the lock key when transmitting and receiving data to and from the other apparatus to make a mutual authentication with the other apparatus to generate a communication key;~~

~~encrypting the communication key with the save key; and~~

~~storing the received data having been encrypted with the communication key corresponding to the communication key encrypted at the encrypting step.~~

Claims 28-35 (Canceled).